



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/086,104	02/26/2002	James Roskind	AOL0022	2741
22862	7590	05/03/2006	EXAMINER	
GLENN PATENT GROUP 3475 EDISON WAY, SUITE L MENLO PARK, CA 94025				ZIA, SYED
		ART UNIT		PAPER NUMBER
		2131		

DATE MAILED: 05/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/086,104	ROSKIND ET AL.
	Examiner Syed Zia	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 13 March 2006.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-15 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-15 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____.
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on March 13, 2006. Original application contained Claims 1-15. Applicant currently amended Claims 1, 5, 7, 9, and 14. The amendment filed on March 13, 2006 have been entered and made of record. Therefore, presently pending claims are 1-15.

Response to Arguments

Applicant did not submit any substantial argument regarding prior art rejection, and stated that newly added limitation is not taught by the Gutman reference. However, this argument with respect to claim 1, 5, 7, 9, and 14 is moot in view of the new ground(s) of rejection. Please refer the rejection below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gutman et al. U. S. Patent 6,298,383, further in view of Purpura (U. S. Patent 6,421,768), hereafter referred to as Purpura.

1. Regarding Claim 1 Gutman teach and describe a distributed network (Fig. 6-8) which is registered with a unique domain name, said network comprising a number of clients and a number of authentication servers, said clients and said authentication servers being communicatively coupled to each other via a global telecommunication network, each of said authentication servers having a fully qualified domain name which is a local host name with said unique domain name appended (col.4 line 20 to line 52),
a distributed authentication system, wherein a given user enters a global user identification (GUID) and a password for authentication to be carried out at a target authentication server, said GUID comprising a user name, a delimitation symbol, and a domain portion which is same as the local host name of said target authentication server (col.7 line 62 to col.8 line 35),
said distributed authentication system comprising: means for parsing an entered GUID and extracting said domain portion therefrom; means for appending said unique domain to said domain portion to form a fully qualified domain name (formed FQDN); means for translating said FQDN to an Internet Protocol (IP) address representing said target authentication server; means for sending said user name and password to said target authentication server for authentication (col.8 line 36 to col.9 line 54).

Although the system disclosed by Gutman shows all the features of the claimed limitation, of a distributed authentication service, where the system keys on the domain portion of the global user identification (GUID), parsing the entered GUID, and redirecting the submission to the appropriate authentication server. Thus rather than consulting a global lookup table, the domain portion of the GUID is pre-pended to a central host domain, i.e., the distributed authentication system's domain, and the domain name system (DNS) is consulted to find location of the authentication servers. But Gutman does not specifically disclose servicing of the authentication, such as password checking, distributed among the participants of the authentication that the system supports.

In an analogous art, Purpura on the other hand discloses computing environment that relates to systems and method for securely transferring user authentication information from a first computer to a second computer to allow the user to seamlessly interact with the second computer without necessarily *re-authenticating* himself thereto.

means for carrying out said authentication at the target authentication server and generating an authentication result that is recognizable by all authentication servers registered in said distributed network; responsive to said generating said authentication result, means for distributing and caching said authentication result (col. 2 line 17 to line 44, col.3 line 38 to line 48, and col.5 line 45 to line 62).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Gutman and Purpura, because Purpura's system of access management for user authentication information from a first computer to one or more other computers to allow the user to interact with the other computers without necessarily having to

explicitly identify himself would not only provide distributed single authentication valid on federated system of servers but would also make the authentication of user in distributed environment more secure because authentication service of proposed system, DNS look-up will not be centrally monitored thus will not consulted a global look-up table to find the location of the underlying authentication servers (Purpura: col.2 line 15 to line 65).

2. Regarding Claim 5 Gutman teach and describe a method for providing distributed authentication service (Fig. 6-13), wherein a given user enters a global user identification (GUID) and a password for authentication to be carried out at a target authentication server, said GUID comprising a user name, a delimitation symbol, and a domain portion which is same as the local host name of said target authentication server (col.7 line 62 to col.8 line 35), said method comprising the computer-implemented steps of: entering the user's GUID and password; parsing said entered GUID and extracting said domain portion from said GUID; appending a unique domain name to said domain portion to form a fully qualified domain name (FQDN); looking up said FQDN in a domain name system (DNS) to obtain an address representing said target authentication server; sending said user name and password to said target authentication server for authentication; carrying out said authentication at the target authentication server and generating an authentication result that is recognizable by all authentication servers registered in said distributed network; responsive to said generating said authentication result (col.7 line 62 to col.8 line 35).

Although the system disclosed by Gutman shows all the features of the claimed limitation, of a distributed authentication service, where the system keys on the domain portion of the global user identification (GUID), parsing the entered GUID, and redirecting the submission to the appropriate authentication server. Thus rather than consulting a global lookup table, the domain portion of the GUID is pre-pended to a central host domain, i.e., the distributed authentication system's domain, and the domain name system (DNS) is consulted to find location of the authentication servers. But Gutman does not specifically disclose servicing of the authentication, such as password checking, distributed among the participants of the authentication that the system supports.

In an analogous art, Purpura on the other hand discloses computing environment that relates to systems and method for securely transferring user authentication information from a first computer to a second computer to allow the user to seamlessly interact with the second computer without necessarily *re-authenticating* himself thereto.

means for carrying out said authentication at the target authentication server and generating an authentication result that is recognizable by all authentication servers registered in said distributed network; responsive to said generating said authentication result, means for distributing and caching said authentication result (col. 2 line 17 to line 44, col.3 line 38 to line 48, and col.5 line 45 to line 62).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Gutman and Purpura, because Purpura's system of access management for user authentication information from a first computer to one or more other computers to allow the user to interact with the other computers without necessarily having to

explicitly identify himself would not only provide distributed single authentication valid on federated system of servers but would also make the authentication of user in distributed environment more secure because authentication service of proposed system, DNS look-up will not be centrally monitored thus will not consulted a global look-up table to find the location of the underlying authentication servers (Purpura: col.2 line 15 to line 65).

3. Regarding Claim 7 Gutman teach and describe a distributed network which is registered with a unique domain name, said network (Fig. 6-8), comprising a number of clients and a number of authentication servers, said clients and said authentication servers being communicatively coupled to each other via a global telecommunications network, each of said authentication servers having a fully qualified domain name which is a local host name with said unique domain name appended (col.4 line 20 to line 52),
a method for providing distributed authentication service, wherein a given user enters a global user identification (GUID) and a password for authentication to be carried out at a target authentication server, said GUID comprising a user name, a delimitation symbol and a domain portion which is same as the local host name of said target authentication server (col.7 line 62 to col.8 line 35),
said method comprising the steps of: entering the user's GUID and password; parsing entered GUID and extracting said domain portion from said GUID; appending said unique domain name to said domain portion to form a fully qualified domain name (FQDN); checking a local list of registered fully qualified domain names (FQDN) to obtain an Internet Protocol (IP) address for

said target authentication server, wherein each FQDN in said local list is mapped to a unique IP address; sending said user name and password to said target authentication server for authentication; carrying out said authentication at the target authentication server and generating an authentication result that is recognizable by all authentication servers registered in said distributed network; and responsive to said generating said authentication result (col.8 line 36 to col.9 line 54).

Although the system disclosed by Gutman shows all the features of the claimed limitation, of a distributed authentication service, where the system keys on the domain portion of the global user identification (GUID), parsing the entered GUID, and redirecting the submission to the appropriate authentication server. Thus rather than consulting a global lookup table, the domain portion of the GUID is pre-pended to a central host domain, i.e., the distributed authentication system's domain, and the domain name system (DNS) is consulted to find location of the authentication servers. But Gutman does not specifically disclose servicing of the authentication, such as password checking, distributed among the participants of the authentication that the system supports.

In an analogous art, Purpura on the other hand discloses computing environment that relates to systems and method for securely transferring user authentication information from a first computer to a second computer to allow the user to seamlessly interact with the second computer without necessarily *re-authenticating* himself thereto.

means for carrying out said authentication at the target authentication server and generating an authentication result that is recognizable by all authentication servers registered in said distributed network; responsive to said generating said authentication result, means for

distributing and caching said authentication result (col. 2 line 17 to line 44, col.3 line 38 to line 48, and col.5 line 45 to line 62).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Gutman and Purpura, because Purpura's system of access management for user authentication information from a first computer to one or more other computers to allow the user to interact with the other computers without necessarily having to explicitly identify himself would not only provide distributed single authentication valid on federated system of servers but would also make the authentication of user in distributed environment more secure because authentication service of proposed system, DNS look-up will not be centrally monitored thus will not consulted a global look-up table to find the location of the underlying authentication servers (Purpura: col.2 line 15 to line 65).

4. Regarding Claim 9 Gutman teach and describe a distributed network which is registered with a unique domain name (Fig. 6-8), said network comprising a number of clients and a number of authentication servers, said clients and said authentication servers being communicatively coupled to each other via a global telecommunications network, each of said authentication servers having a fully qualified domain name which is a local host name with said unique domain name appended (col.4 line 20 to line 52),
a method for providing distributed authentication service, wherein a given user enters a global user identification (GUID) and a password for authentication to be carried out at a target authentication server, said GUID comprising a user name, a delimitation symbol and a domain

portion which is same as the local host name of said target authentication server (col.7 line 62 to col.8 line 35),

said method comprising the computer-implemented steps of: entering the user's GUID and password; parsing said GUID and extracting said domain portion; appending said unique domain name to said domain portion to form a fully qualified domain name (FQDN) in said unique domain; checking a local list of registered fully qualified domain names (RFQDN) to obtain an Internet Protocol (IP) address for said target authentication server, wherein each RFQDN in said local list is mapped to a unique IP address; if said step of checking fails, looking up a domain name system (DNS) to obtain an Internet Protocol (IP) address representing said FQDN; sending said user name and password to said target authentication server for authentication; carrying out said authentication at the target authentication server and generating an authentication result that is recognizable by all authentication servers registered in said distributed network; and responsive to said generating said authentication result (col.8 line 36 to col.9 line 54).

Although the system disclosed by Gutman shows all the features of the claimed limitation, of a distributed authentication service, where the system keys on the domain portion of the global user identification (GUID), parsing the entered GUID, and redirecting the submission to the appropriate authentication server. Thus rather than consulting a global lookup table, the domain portion of the GUID is pre-pended to a central host domain, i.e., the distributed authentication system's domain, and the domain name system (DNS) is consulted to find location of the authentication servers. But Gutman does not specifically disclose servicing of the authentication, such as password checking, distributed among the participants of the authentication that the system supports.

In an analogous art, Purpura on the other hand discloses computing environment that relates to systems and method for securely transferring user authentication information from a first computer to a second computer to allow the user to seamlessly interact with the second computer without necessarily *re-authenticating* himself thereto.

means for carrying out said authentication at the target authentication server and generating an authentication result that is recognizable by all authentication servers registered in said distributed network; responsive to said generating said authentication result, means for distributing and caching said authentication result (col. 2 line 17 to line 44, col.3 line 38 to line 48, and col.5 line 45 to line 62).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Gutman and Purpura, because Purpura's system of access management for user authentication information from a first computer to one or more other computers to allow the user to interact with the other computers without necessarily having to explicitly identify himself would not only provide distributed single authentication valid on federated system of servers but would also make the authentication of user in distributed environment more secure because authentication service of proposed system, DNS look-up will not be centrally monitored thus will not consulted a global look-up table to find the location of the underlying authentication servers (Purpura: col.2 line 15 to line 65).

5. Regarding Claim 11 Gutman teach and describe a method for providing distributed authentication service (Fig. 6-13), wherein a given user enters a global user identification

(GUID) and a password for authentication to be carried out at a target authentication server, said GUID comprising a user name, a delimitation symbol and said target authentication server's domain name (col.7 line 62 to col.8 line 35), said method comprising the steps of: entering the user's GUID and password; parsing said entered GUID and extracting said target authentication server's domain name; pre-pending said common local host name to said target authentication server's domain name to form a fully qualified domain name (FQDN); checking a local list of registered fully qualified domain names (RFQDN) to obtain an address for said target authentication server, wherein each RFQDN in said local is mapped to a unique address; sending said user name and password to said target authentication server for authentication; carrying out said authentication at the target authentication server and generating an authentication result that is recognizable by all authentication servers registered in said distributed network; and responsive to said generating said authentication result (col.8 line 36 to col.9 line 54).

Although the system disclosed by Gutman shows all the features of the claimed limitation, of a distributed authentication service, where the system keys on the domain portion of the global user identification (GUID), parsing the entered GUID, and redirecting the submission to the appropriate authentication server. Thus rather than consulting a global lookup table, the domain portion of the GUID is pre-pended to a central host domain, i.e., the distributed authentication system's domain, and the domain name system (DNS) is consulted to find location of the authentication servers. But Gutman does not specifically disclose servicing of the authentication, such as password checking, distributed among the participants of the authentication that the system supports.

In an analogous art, Purpura on the other hand discloses computing environment that relates to systems and method for securely transferring user authentication information from a first computer to a second computer to allow the user to seamlessly interact with the second computer without necessarily *re-authenticating* himself thereto.

means for carrying out said authentication at the target authentication server and generating an authentication result that is recognizable by all authentication servers registered in said distributed network; responsive to said generating said authentication result, means for distributing and caching said authentication result (col. 2 line 17 to line 44, col.3 line 38 to line 48, and col.5 line 45 to line 62).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Gutman and Purpura, because Purpura's system of access management for user authentication information from a first computer to one or more other computers to allow the user to interact with the other computers without necessarily having to explicitly identify himself would not only provide distributed single authentication valid on federated system of servers but would also make the authentication of user in distributed environment more secure because authentication service of proposed system, DNS look-up will not be centrally monitored thus will not consulted a global look-up table to find the location of the underlying authentication servers (Purpura: col.2 line 15 to line 65).

6. Regarding Claim 14 Gutman teach and describe a distributed network comprising a number of clients and a number of authentication servers (Fig. 6-8), said clients and said

authentication servers being communicatively coupled to each other via a global telecommunications network, each of said authentication servers having a fully qualified domain name which is a local host name with its domain name appended (col.4 line 20 to line 52), a method for providing distributed authentication service, wherein a given user enters a global user identification (GUID) and a password for authentication to be carried out at a target authentication server, said GUID comprising a user name, a delimitation symbol and said target authentication server's domain name (col.7 line 62 to col.8 line 35), said method comprising the steps of: entering the user's GUID and password; parsing said entered GUID and extracting said target authentication server's domain name; checking a local list of domain names to obtain an Internet Protocol (IP) address for said target authentication server, wherein each domain name in said list is mapped to a registered authentication server's IP address; sending said user name and password to said target authentication server for authentication; carrying out said authentication at the target authentication server and generating an authentication result that is recognizable by all authentication servers registered in said distributed network; responsive to said generating said authentication result (col.8 line 36 to col.9 line 54).

Although the system disclosed by Gutman shows all the features of the claimed limitation, of a distributed authentication service, where the system keys on the domain portion of the global user identification (GUID), parsing the entered GUID, and redirecting the submission to the appropriate authentication server. Thus rather than consulting a global lookup table, the domain portion of the GUID is pre-pended to a central host domain, i.e., the distributed authentication system's domain, and the domain name system (DNS) is consulted to find location

of the authentication servers. But Gutman does not specifically disclose servicing of the authentication, such as password checking, distributed among the participants of the authentication that the system supports.

In an analogous art, Purpura on the other hand discloses computing environment that relates to systems and method for securely transferring user authentication information from a first computer to a second computer to allow the user to seamlessly interact with the second computer without necessarily *re-authenticating* himself thereto.

means for carrying out said authentication at the target authentication server and generating an authentication result that is recognizable by all authentication servers registered in said distributed network; responsive to said generating said authentication result, means for distributing and caching said authentication result (col. 2 line 17 to line 44, col.3 line 38 to line 48, and col.5 line 45 to line 62).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Gutman and Purpura, because Purpura's system of access management for user authentication information from a first computer to one or more other computers to allow the user to interact with the other computers without necessarily having to explicitly identify himself would not only provide distributed single authentication valid on federated system of servers but would also make the authentication of user in distributed environment more secure because authentication service of proposed system, DNS look-up will not be centrally monitored thus will not consulted a global look-up table to find the location of the underlying authentication servers (Purpura: col.2 line 15 to line 65).

7. Regarding Claims 2-4, 6, 8, 10, 12-13, and 15 are rejected applied as above rejecting Claims 1, 5, 7, 9, 11, and 14. Furthermore, the system of Gutman and Purpura teaches and describes a distributed authentication system, wherein:

As per Claim 2, further comprising: means for automatically mapping any unrecognized FQDN into a default server which carries out authentication on the user's authentication request (col. 9 line 32 to line 54).

As per Claim 3, said means for translating consults a domain name system (DNS) to obtain an Internet Protocol (IP) address representing said target authentication server (col.5 line 1 to line 37).

As per Claim 4, said means for translating consults a local mapping list to obtain an Internet Protocol (IP) address representing said target authentication server (col.5 line 1 to line 17).

As per Claim 6, 8, and 10 further comprising the steps of: if said step of looking up fails, automatically mapping an unrecognized FQDN into a default server which performs authentication on the user's authentication request (col.9 line 16 to col.10 line 11).

As per Claim 12, further comprising the step of: if said step of checking fails, looking up said FQDN in a domain name system (DNS) to obtain an address representing said target authentication server (col.9 line 16 to col.10 line 11).

As per Claim 13, further comprising the steps of: if said step of looking up fails, automatically mapping an unrecognized FQDN into a default server which performs authentication on the user's authentication request (col.9 line 16 to col.10 line 11).

As per Claim 15, further comprising the step of: if said step of checking fails, automatically mapping an unrecognized domain name into a default server which performs authentication on the user's authentication request (col.9 line 16 to col.10 line 11).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



sz
April 03, 2006